Aon Service Corporation
Law | Global Privacy Office

Aon Client Data Privacy Summary

Empower Results®

Table of Contents

Our Commitment to Data Privacy

Data Privacy Backdrop

As organisations seek to improve their customer and employee experience, create value, and obtain a competitive advantage, the ability to manage data privacy risks and demonstrate compliance with emerging data privacy laws is imperative.

Our Commitment

Our commitment to integrity extends to the personal information we collect, process, and store on behalf of our clients and business partners. In particular, we are committed to ensuring that any personal information entrusted to us is afforded an appropriate level of security protection and is only used in a way that our clients' customers and employees would reasonably expect.

How We Manage Data Privacy

We take data privacy extremely seriously and we have invested significant resources into the development of a framework to ensure that our core products and services are compliant with applicable data privacy laws and that wider data privacy risks are effectively managed.

Our approach:

- starts with our Code of Business Conduct, which sets out senior management commitment to comply with data privacy laws in all the jurisdictions in which we do business and the standards of behaviour expected of our people when working with each other, our clients, and our business partners;
- is underpinned and supported by appropriate data privacy policies, standards, and standard operating procedures that have been specifically designed to ensure that data privacy risks are effectively managed across our businesses;
- is driven by our Chief Privacy Officer and Global Privacy Office, who are responsible for promoting compliance and awareness of applicable data privacy laws, advising on the implementation of our data privacy policies and standards, and monitoring compliance in jurisdictions across the globe
- focuses on establishing a sustainable data privacy control framework which places sufficient emphasis on the implementation and continual improvement of effective data privacy control.

Our Data Privacy Principles

Our approach to managing data privacy risks is grounded across a number of areas, which are summarised below.

Strategy & Governance

- We have established a Global Privacy Office (the "GPO"), which is led by the Chief Privacy Officer who reports to the Board as well as an Executive Committee. The GPO comprises a number of full-time privacy professionals located around the globe and is responsible for implementing Aon's data privacy program, designing and developing data privacy compliance solutions, and supporting our global data privacy champion network.
- We have appointed a number of data privacy champions across our businesses that are responsible for ensuring that our data privacy policies, standards and procedures are implemented across our business areas and are operating effectively.

Information Security

- Our strategic data security approach is to build controls to protect, detect, respond to, and recover from adverse cyber and information security events.
- We maintain a suite of data and cyber security policies that set out our commitment and expectations for the protection and security of personal information.
- We implement a security awareness and training program to raise our colleagues' awareness of their responsibilities for the protection of personal data.
- We operate a global security operations centre to monitor, detect, manage and respond to security incidents, including any cyber threats to our network and systems.

Data Lifecycle Management

- We maintain appropriate records of our processing activities involving personal information, which will provide us with a view of where we collect, use, retain, and disclose personal information across our business globally. These processing records have been designed to enable us to meet our data privacy legal and regulatory obligations (e.g., New York Department of Financial Services Cyber Regulations, GDPR, etc.).
- We have implemented appropriate procedures to ensure our processing records are reviewed periodically.
- We have processes in place to help us determine our legal basis for processing (e.g., legitimate interests; consent): we leverage our data inventory to document our view of our processing and take steps to ensure we have the corresponding notice and consent tracking actions in place where required.

Privacy by Design (PbD)

- Privacy Impact Assessments: We maintain procedures to ensure projects involving personal information undergo review prior to implementation to ensure data privacy risks posed to individuals are identified and effectively managed.
- Data Minimisation: We have mechanisms to help ensure personal information we collect from our clients is restricted to the minimum we need to provide our services.
- Data Retention: We adopt data retention standards and schedules establishing the limits on retaining client data.
- Data Destruction: We have processes to securely erase data in accordance with our retention standards.

Privacy Incident Management

- We take a multidisciplinary, holistic incident response approach. This approach is reviewed and updated on a regular basis to help ensure that it incorporates changes in applicable laws and regulations (e.g., GDPR).
- We have robust processes in place to ensure that incidents are identified and responded to effectively.
- We track and monitor potential incidents and undertake root cause analyses to help minimise the risk of similar potential issues occurring in the future.

Regulatory Change

- We keep abreast of updates in the data privacy legal and regulatory landscape, particularly where there may be changes that impact our global businesses. We undertake impact assessments to determine what impact those changes may have on our personal information processing activities.
- We send out newsletters across our internal data privacy network to ensure individuals have accurate and up-to-date knowledge of data privacy legal and regulatory changes and Aon's response to addressing them.

Data Processor Accountability

- Pre-Contract: We undertake due diligence of third parties with whom we engage to ensure that their privacy environment meets our expectations in line with our legal, regulatory and contractual commitments and obligations.
- Contract: We adopt a robust contractual framework methodology with appropriate privacy clauses in line with applicable legal requirements.
- On-going assurance: We have an on-going assurance programme which assesses third party vendors against our data privacy and security requirements.

Risk and Control

- We have appropriate processes in place to identify data privacy risks commensurate with our legal and regulatory obligations.
- We design, develop, and implement risk-justified controls to ensure data privacy risks are effectively managed.
- To ensure accountability we review these controls regularly to make sure they are implemented correctly and are operating effectively.

Training and Awareness

- Our colleagues are required to complete global privacy training, which sets out Aon's expectations and requirements in the handling of personal information.
- We require certain colleagues to complete role specific or country specific training if there are specific actions we expect them to undertake.
- We conduct regular awareness campaigns and ad-hoc training roadshows to reinforce key training messages.

Policy Management

- We have in place a Global Privacy Policy to provide a clear framework for setting data privacy objectives across our business and to set the minimum standards and internal controls that must be adhered to by our colleagues when handling personal information.
- Our Global Privacy Policy is communicated to colleagues as part of their data privacy training and within our Code of Business Conduct, which is reaffirmed by Aon colleagues on an annual basis.
- Our externally facing privacy statements provide transparency of our data processing activities. .

Individual Rights Processing

- Data Subject Rights: We have in place standard operating procedures to ensure we take a consistent and rigorous approach, in line with our legal and contractual obligations, to managing requests from individuals to exercise their rights under data protection laws (including, for example, rights of access, rectification, erasure and objection to processing).

Cross-Border Data Strategy

- We review all of our global processes and apply a consistent and rigorous approach to the management of how personal data is used and stored globally.
- We implement appropriate agreements with our vendors and group legal entities which incorporate EU standard contractual clauses where appropriate to legitimise the processing of personal information undertaken across Aon globally.

Monitoring

- At the core of our approach to data privacy is the need to undertake on-going and sustainable monitoring of our processes and procedures to help ensure that the activities which we undertake are appropriately addressed.
- Where issues are identified we have processes in place to report, respond to, remediate, and document those issues.

Contact Information

Global Privacy Office
privacy@aon.com

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.